

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE DIVISION

STEVEN HORN, individually and  
on behalf of all others similarly  
situated,

*Plaintiff,*

v.

AMAZON.COM, INC.,

*Defendant.*

CASE NO. 2:23-cv-01727-RSL

**ORDER REGARDING  
DISCOVERY OF  
ELECTRONICALLY STORED  
INFORMATION**

The Court hereby establishes the following provisions regarding the discovery of electronically stored information (“ESI”) in this matter:

**A. General Principles**

1. An attorney’s zealous representation of a client is not compromised by conducting discovery in a cooperative manner. The failure of counsel or the parties to litigation to cooperate in facilitating and reasonably limiting discovery requests and responses raises litigation costs and contributes to the risk of sanctions.

2. As provided in LCR 26(f), the proportionality standard set forth in Fed. R. Civ. P. 26(b)(1) must be applied in each case when formulating a discovery plan. To further the application of the proportionality standard in discovery, requests for production of ESI and related

1 responses should be reasonably targeted, clear, and as specific as possible. This order is intended  
2 to assist the parties in identifying relevant, responsive information that has been stored  
3 electronically and is proportional to the needs of the case. The order does not supplant the parties'  
4 obligations to comply with Fed. R. Civ. P. 34.

5 **B. ESI Disclosures**

6 Within 30 days of entry of this Order, or at a later time if agreed to by the parties, each  
7 party shall disclose:

8 1. Custodians. The custodians most likely to have discoverable ESI in their  
9 possession, custody, or control. The custodians shall be identified by name, title, connection to  
10 the instant litigation, and the type of the information under the custodian's control.

11 2. Non-custodial Data Sources. A list of non-custodial data sources (*e.g.*, shared  
12 drives, servers), if any, likely to contain discoverable ESI.

13 3. Third-Party Data Sources. A list of third-party data sources, if any, likely to  
14 contain discoverable ESI (*e.g.*, third-party email providers, mobile device providers, cloud  
15 storage) and, for each such source, the extent to which a party is (or is not) able to preserve  
16 information stored in the third-party data source.

17 4. Inaccessible Data. A list of data sources, if any, likely to contain discoverable ESI  
18 (by type, date, custodian, electronic system or other criteria sufficient to specifically identify the  
19 data source) that a party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B).

20 5. Foreign data privacy laws. Nothing in this Order is intended to prevent either party  
21 from complying with the requirements of a foreign country's data privacy laws, *e.g.*, the European  
22 Union's General Data Protection Regulation (GDPR) (EU) 2016/679. The parties shall meet and  
23  
24  
25

1 confer before including custodians or data sources subject to such laws in any ESI or other  
2 discovery request.

3 **C. ESI Discovery Procedures**

4 1. On-site inspection of electronic media. Such an inspection shall not be required  
5 absent a demonstration by the requesting party of specific need and good cause or by agreement  
6 of the parties.

7 2. Search methodology. The parties shall timely confer to attempt to reach agreement  
8 on appropriate search terms and queries, file type and date restrictions, data sources (including  
9 custodians), and other appropriate computer- or technology-aided methodologies, before any such  
10 effort is undertaken. The parties shall continue to cooperate in revising the appropriateness of the  
11 search methodology.

12 a. Prior to running searches:

13 i. The producing party shall disclose the data sources (including  
14 custodians), search terms and queries, any file type and date restrictions, and any other  
15 methodology that it proposes to use to locate ESI likely to contain responsive and discoverable  
16 information. The producing party may provide unique hit counts for each search query.

17 ii. After disclosure, the parties will engage in a meet and confer  
18 process regarding additional terms sought by the non-producing party.

19 iii. The following provisions apply to search terms / queries of the  
20 requesting party. Focused terms and queries should be employed; broad terms or queries, such  
21 as product and company names, generally should be avoided. A conjunctive combination of  
22 multiple words or phrases (*e.g.*, “computer” and “system”) narrows the search and shall count as  
23 a single search term. A disjunctive combination of multiple words or phrases (*e.g.*, “computer”  
24  
25

1 or “system”) broadens the search, and thus each word or phrase shall count as a separate search  
2 term unless they are variants of the same word. The producing party may identify each search  
3 term or query returning overbroad results demonstrating the overbroad results and a counter  
4 proposal correcting the overbroad search or query. .

5 c. Upon reasonable request, a party shall disclose information relating to  
6 network design, the types of databases, database dictionaries, the access control list and security  
7 access logs and rights of individuals to access the system and specific files and applications, the  
8 ESI document retention policy, organizational chart for information systems personnel, or the  
9 backup and systems recovery routines, including, but not limited to, tape rotation and  
10 destruction/overwrite policy.

11 3. Format.

12 a. ESI will be produced to the requesting party with searchable text, in a  
13 format to be decided between the parties. Acceptable formats include, but are not limited to, native  
14 files, multi-page TIFFs (with a companion OCR or extracted text file), single-page TIFFs (only  
15 with load files for e-discovery software that includes metadata fields identifying natural document  
16 breaks and also includes companion OCR and/or extracted text files), and searchable PDF.

17 b. Unless otherwise agreed to by the parties, files that are not easily converted  
18 to image format, such as spreadsheet, database, and drawing files, will be produced in native  
19 format.

20 c. Each document image file shall be named with a unique number (Bates  
21 Number). File names should not be more than twenty characters long or contain spaces. When a  
22 text-searchable image file is produced, the producing party must preserve the integrity of the  
23  
24  
25

1 underlying ESI, *i.e.*, the original formatting, the metadata (as noted below) and, where applicable,  
2 the revision history.

3 d. If a document is more than one page, the unitization of the document and  
4 any attachments and/or affixed notes shall be maintained as they existed in the original document.

5 e. The full text of each electronic document shall be extracted (“Extracted  
6 Text”) and produced in a text file. The Extracted Text shall be provided in searchable ASCII text  
7 format (or Unicode text format if the text is in a foreign language) and shall be named with a  
8 unique Bates Number (*e.g.*, the unique Bates Number of the first page of the corresponding  
9 production version of the document followed by its file extension).

10 4. De-duplication. The parties may de-duplicate their ESI production across custodial  
11 and non-custodial data sources after disclosure to the requesting party, and the duplicate custodian  
12 information removed during the de-duplication process tracked in a duplicate/other custodian  
13 field in the database load file.

14 5. Email Threading. The parties may use analytics technology to identify email  
15 threads and need only produce the unique most inclusive copy and related family members and  
16 may exclude lesser inclusive copies. Upon reasonable request, the producing party will produce  
17 a less inclusive copy.

18 6. Metadata fields. If the requesting party seeks metadata, only the following  
19 metadata fields need be produced, and only to the extent it is reasonably accessible and non-  
20 privileged: document type; custodian and duplicate custodians (or storage location if no  
21 custodian); author/from; recipient/to, cc and bcc; title/subject; email subject; file name; file size;  
22 file extension; original file path; date and time created, sent, modified and/or received; and hash  
23 value. The list of metadata type is intended to be flexible and may be changed by agreement of  
24

1 the parties, particularly in light of advances and changes in technology, vendor, and business  
2 practices.

3 **D. Preservation of ESI**

4 The parties have a common law obligation, as expressed in Fed. R. Civ. P. 37(e), to take  
5 reasonable and proportional steps to preserve discoverable information in the party's possession,  
6 custody, or control. With respect to preservation of ESI:

7 1. Absent a showing of good cause by the requesting party, the parties shall not be  
8 required to modify the procedures used by them in the ordinary course of business to back-up and  
9 archive data; provided, however, that the parties shall preserve all discoverable ESI in their  
10 possession, custody, or control.

11 2. The parties will supplement their disclosures in accordance with Fed. R. Civ. P.  
12 26(e) with discoverable ESI responsive to a particular discovery request or mandatory disclosure  
13 where that data is created after a disclosure or response is made (unless excluded under Sections  
14 (D)(3) or (E)(1)-(2)).

15 3. Absent a showing of good cause by the requesting party, the following categories  
16 of ESI need not be preserved:

- 17 a. Deleted, slack, fragmented, or other data only accessible by forensics.
- 18 b. Random access memory (RAM), temporary files, or other ephemeral data  
19 that are difficult to preserve without disabling the operating system.
- 20 c. On-line access data such as temporary internet files, history, cache,  
21 cookies, and the like.
- 22 d. Data in metadata fields that are frequently updated automatically, such as  
23 last-opened dates (see also Section (E)(5)).
- 24 e. Back-up data that are duplicative of data that are more accessible  
25 elsewhere.
- 26 f. Server, system or network logs.

g. Data remaining from systems no longer in use that is unintelligible on the systems in use.

h. Electronic data (*e.g.*, email, calendars, contact data, and notes) sent to or from mobile devices (*e.g.*, iPhone, iPad, Android devices), provided that a copy of all such electronic data is automatically saved in real time elsewhere (such as on a server, laptop, desktop computer, or “cloud” storage).

**E. Privilege**

1. A producing party shall create a privilege log of all documents fully withheld from production on the basis of a privilege or protection, unless otherwise excepted by this Order. Privilege logs shall include a unique identification number for each document and the basis for the claim (attorney-client privileged or work-product protection). For ESI, the privilege log may be generated using available metadata, including author/recipient or to/from/cc/bcc names; the subject matter or title; and date created. Should the available metadata provide insufficient information for the purpose of evaluating the privilege claim asserted, the producing party shall include such additional information as required by the Federal Rules of Civil Procedure. Privilege logs will be produced to all other parties no later than 30 days after delivering a production unless an earlier deadline is agreed to by the parties.

2. Redactions need not be logged so long as the basis for the redaction is clear on the redacted document.

3. With respect to privileged or work-product information generated after the filing of the complaint, parties are not required to include any such information in privilege logs.

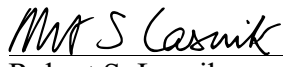
4. Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Fed. R. Civ. P. 26(b)(3)(A) and (B).

5. Pursuant to Fed. R. Evid. 502(d), the production of any documents, electronically stored information (ESI) or information, whether inadvertent or otherwise, in this proceeding

1 shall not, for the purposes of this proceeding or any other federal or state proceeding, constitute  
2 a waiver by the producing party of any privilege applicable to those documents, including the  
3 attorney-client privilege, attorney work-product protection, or any other privilege or protection  
4 recognized by law. This Order shall be interpreted to provide the maximum protection allowed  
5 by Fed. R. Evid. 502(d). The provisions of Fed. R. Evid. 502(b) do not apply. Nothing contained  
6 herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI  
7 or information (including metadata) for relevance, responsiveness and/or segregation of  
8 privileged and/or protected information before production. Information produced in discovery  
9 that is protected as privileged or work product shall be immediately returned to the producing  
10 party.

11 IT IS SO ORDERED.

12 Dated this 27<sup>th</sup> day of January, 2025.

13   
14 Robert S. Lasnik  
15 US District Judge  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25